EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	5	(((authenticat$3 adj5 (value or number or identifier)) near5 (compar$3 or match$3)) and (integrity adj5 message)).clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/09 11:57
L2	306	380/247.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/09 11:55
L3	421	380/255.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/09 11:55
L4	0	370/12.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/09 11:55
L5	1284	370/445.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/09 11:56
L6	165	726/18.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/09 11:56
L7	298	726/19.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/09 11:56
L8	1660	713/168.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/09 11:57
L9	378	713/181.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/09 11:57

EAST Search History

L10	0	(l2 or l3 or l5 or l6 or l7 or l8 or l9) and (((authenticat$3 adj5 (value or number or identifier)) near5 (compar$3 or match$3)) same (integrity adj5 message))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/09 11:58
L11	5	(((authenticat$3 adj5 (value or number or identifier)) near5 (compar$3 or match$3)) same (integrity adj5 message))	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/09 11:58

PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

+"message integrity"; +"authentication value" SEARCH

Feedback Report a problem Satisfaction survey

Terms used **authentication value**

Found **3** of **198,310**

Sort results by: relevance
Display results: expanded form

Save results to a Binder
Search Tips
□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 3 of 3

Relevance scale

1 Group Key Management and Signatures: Provably authenticated group Diffie-Hellman key exchange
Emmanuel Bresson, Olivier Chevassut, David Pointcheval, Jean-Jacques Quisquater
November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security CCS '01**
Publisher: ACM Press
Full text available: pdf(578.14 KB) Additional Information: full citation, abstract, references, citings, index terms

Group Diffie-Hellman protocols for Authenticated Key Exchange (AKE) are designed to provide a pool of players with a shared secret key which may later be used, for example, to achieve multicast message integrity. Over the years, several schemes have been offered. However, no formal treatment for this cryptographic problem has ever been suggested. In this paper, we present a security model for this problem and use it to precisely define AKE (with "implicit" authentication) as the fundamental goal ...

2 SPINS: security protocols for sensor netowrks
Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar
July 2001 **Proceedings of the 7th annual international conference on Mobile computing and networking MobiCom '01**
Publisher: ACM Press
Full text available: pdf(242.17 KB) Additional Information: full citation, abstract, references, citings, index terms

As sensor networks edge closer towards wide-spread deployment, security issues become a central concern. So far, much research has focused on making sensor networks feasible and useful, and has not concentrated on security.

We present a suite of security building blocks optimized for resource-constrained environments and wireless communication. SPINS has two secure building blocks: SNEP and &mgr;TESLA SNEP provides the following important baseline security primitives: Data confidentia ...

3 SPINS: security protocols for sensor networks
Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler
September 2002 **Wireless Networks**, Volume 8 Issue 5
Publisher: Kluwer Academic Publishers
Full text available: pdf(213.37 KB) Additional Information: full citation, abstract, references, citings, index terms

Wireless sensor networks will be widely deployed in the near future. While much research has focused on making these networks feasible and useful, security has received little attention. We present a suite of security protocols optimized for sensor networks: SPINS. SPINS has two secure building blocks: SNEP and μTESLA. SNEP includes: data confidentiality, two-party data authentication, and evidence of data freshness. μTESLA provides authenticated broadcast for severely resource-constrained ...

Keywords: MANET, authentication of wireless communication, cryptography, mobile ad hoc networks, secrecy and confidentiality, secure communication protocols, sensor networks

Results 1 - 3 of 3

PORTAL

USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

+message; +integrity; +"authentication value" SEARCH

Feedback Report a problem Satisfaction survey

Terms used **message; integrity; authentication value**

Found **10** of **198,310**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 10 of 10

Relevance scale

1 Authentication and integrity in outsourced databases

Einar Mykletun, Maithili Narasimha, Gene Tsudik
May 2006 **ACM Transactions on Storage (TOS)**, Volume 2 Issue 2
Publisher: ACM Press
Full text available: pdf(531.47 KB) Additional Information: full citation, abstract, references, index terms

In the Outsourced Database (ODB) model, entities outsource their data management needs to a third-party service provider. Such a service provider offers mechanisms for its clients to create, store, update, and access (query) their databases. This work provides mechanisms to ensure data integrity and authenticity for outsourced databases. Specifically, this article provides mechanisms that assure the querier that the query results have not been tampered with and are authentic (with respect to the ...

Keywords: Outsourced databases, authentication, data authenticity, data integrity, integrity, signature aggregation, storage

2 Main track: Securing the deluge Network programming system

Prabal K. Dutta, Jonathan W. Hui, David C. Chu, David E. Culler
April 2006 **Proceedings of the fifth international conference on Information processing in sensor networks IPSN '06**
Publisher: ACM Press
Full text available: pdf(331.36 KB) Additional Information: full citation, abstract, references, citings, index terms

A number of multi-hop, wireless, network programming systems have emerged for sensor network retasking but none of these systems support a cryptographically-strong, public-key-based system for source authentication and integrity verification. The traditional technique for authenticating a program binary, namely a digital signature of the program hash, is poorly suited to resource-contrained sensor nodes. Our solution to the secure programming problem leverages authenticated streams, is consisten ...

Keywords: authenticated broadcast, dissemination protocols, network programming, security, wireless sensor networks

3 SPINS: security protocols for sensor netowrks

Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar
July 2001 **Proceedings of the 7th annual international conference on Mobile computing and networking MobiCom '01**
Publisher: ACM Press
Full text available: Additional Information: full citation, abstract, references, citings, index

pdf(242.17 KB) terms

As sensor networks edge closer towards wide-spread deployment, security issues become a central concern. So far, much research has focused on making sensor networks feasible and useful, and has not concentrated on security.

We present a suite of security building blocks optimized for resource-constrained environments and wireless communication. SPINS has two secure building blocks: SNEP and &mgr;TESLA SNEP provides the following important baseline security primitives: Data confidentia ...

4 SPINS: security protocols for sensor networks
Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler
September 2002 **Wireless Networks**, Volume 8 Issue 5
Publisher: Kluwer Academic Publishers
Full text available: pdf(213.37 KB) Additional Information: full citation, abstract, references, citings, index terms

Wireless sensor networks will be widely deployed in the near future. While much research has focused on making these networks feasible and useful, security has received little attention. We present a suite of security protocols optimized for sensor networks: SPINS. SPINS has two secure building blocks: SNEP and μTESLA. SNEP includes: data confidentiality, two-party data authentication, and evidence of data freshness. μTESLA provides authenticated broadcast for severely resource-constrained ...

Keywords: MANET, authentication of wireless communication, cryptography, mobile ad hoc networks, secrecy and confidentiality, secure communication protocols, sensor networks

5 SPV: secure path vector routing for securing BGP
Yih-Chun Hu, Adrian Perrig, Marvin Sirbu
August 2004 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '04**, Volume 34 Issue 4
Publisher: ACM Press
Full text available: pdf(236.82 KB) Additional Information: full citation, abstract, references, citings, index terms

As our economy and critical infrastructure increasingly relies on the Internet, the insecurity of the underlying border gateway routing protocol (BGP) stands out as the Achilles heel. Recent misconfigurations and attacks have demonstrated the brittleness of BGP. Securing BGP has become a priority.In this paper, we focus on a viable deployment path to secure BGP. We analyze security requirements, and consider tradeoffs of mechanisms that achieve the requirements. In particular, we study how to se ...

Keywords: BGP, Border Gateway Protocol, interdomain routing, routing, security

6 Formal analysis of card-based payment systems in mobile devices
Vijayakrishnan Pasupathinathan, Josef Pieprzyk, Huaxiong Wang, Joo Yeon Cho
January 2006 **Proceedings of the 2006 Australasian workshops on Grid computing and e-research - Volume 54 ACSW Frontiers '06**
Publisher: Australian Computer Society, Inc.
Full text available: pdf(169.95 KB) Additional Information: full citation, abstract, references, index terms

To provide card holder authentication while they are conducting an electronic transaction using mobile devices, VISA and MasterCard independently proposed two electronic payment protocols: Visa 3D Secure and MasterCard Secure Code. The protocols use pre-registered passwords to provide card holder authentication and Secure Socket Layer/ Transport Layer Security (SSL/TLS) for data confidentiality over wired networks and

Wireless Transport Layer Security (WTLS) between a wireless device and a Wirel ...

Keywords: card-based systems, electronic payments, formal verification, mobile payment

7 Short papers -- works in progress: Secured storage using secureParser™
Sabre A. Schnitzer, Robert A. Johnson, Henry Hoyt
November 2005 **Proceedings of the 2005 ACM workshop on Storage security and survivability StorageSS '05**
Publisher: ACM Press
Full text available: pdf(397.54 KB) Additional Information: full citation, abstract, references, index terms

Securing storage data is a manifold problem with requirements in three dimensions: data security, data integrity, and the safety of data. Meeting the requirements for one dimension often means compromising another. SecureParser™ is a software technology which addresses all three dimensions of secure storage without compromising any. In this paper, we describe the SecureParser™ technology and discuss how it addresses the three dimensions of secured storage: secur ...

Keywords: encryption, fabric, file system, parsing

8 Password Management and Digital Signatures: The BiBa one-time signature and broadcast authentication protocol
Adrian Perrig
November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security CCS '01**
Publisher: ACM Press
Full text available: pdf(268.66 KB) Additional Information: full citation, abstract, references, citings, index terms

We introduce the *BiBa signature* scheme, a new signature construction that uses one-way functions without trapdoors. BiBa features a low verification overhead and a relatively small signature size. In comparison to other one-way function based signature schemes, BiBa has smaller signatures and is at least twice as fast to verify (which probably makes it one of the fastest signature scheme to date for verification). On the downside, the BiBa public key is large, and the signature generation ...

Keywords: broadcast authentication, one-time signature, signature based on a one-way function without trapdoor, source authentication for multicast

9 Group Key Management and Signatures: Provably authenticated group Diffie-Hellman key exchange
Emmanuel Bresson, Olivier Chevassut, David Pointcheval, Jean-Jacques Quisquater
November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security CCS '01**
Publisher: ACM Press
Full text available: pdf(578.14 KB) Additional Information: full citation, abstract, references, citings, index terms

Group Diffie-Hellman protocols for Authenticated Key Exchange (AKE) are designed to provide a pool of players with a shared secret key which may later be used, for example, to achieve multicast message integrity. Over the years, several schemes have been offered. However, no formal treatment for this cryptographic problem has ever been suggested. In this paper, we present a security model for this problem and use it to precisely define AKE (with "implicit" authentication) as the fundamental goal ...

10 Privacy and authentication: Fourth-factor authentication: somebody you know
John Brainard, Ari Juels, Ronald L. Rivest, Michael Szydlo, Moti Yung

October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press
Full text available: pdf(372.40 KB) Additional Information: full citation, abstract, references, index terms

User authentication in computing systems traditionally depends on three factors: something you have (e.g., a hardware token), something you are (e.g., a fingerprint), and something you know (e.g., a password). In this paper, we explore a fourth factor, the social network of the user, that is, somebody you know.Human authentication through mutual acquaintance is an age-old practice. In the arena of computer security, it plays roles in privilege delegation, peer-level certification, help-desk assi ...

Keywords: authentication, hardware tokens, vouchers

Results 1 - 10 of 10

IEEE Xplore® RELEASE 2.2

Home | Login | Logout | Access Information | Alerts |

Welcome United States Patent and Trademark Office

Search Results

BROWSE SEARCH IEEE XPLORE GUIDE

Results for "**((authentication value<in>metadata) <and> (integrity<in>metadata))**"
Your search matched **1** of **1516137** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

e-mail

» **Search Options**

View Session History

New Search

Modify Search

((authentication value<in>metadata) <and> (integrity<in>metadata)) Search

□ Check to search only within this results set

Display Format: ● Citation ○ Citation & Abstract

view selected items **Select All** **Deselect All**

» **Key**

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

□ 1. **CryptoPage: An Efficient Secure Architecture with Memory Encryption, Ir Information Leakage Protection**
Duc, G.; Keryell, R.;
Computer Security Applications Conference, 2006. ACSAC '06. 22nd Annual
Dec. 2006 Page(s):483 - 492
Digital Object Identifier 10.1109/ACSAC.2006.21
AbstractPlus | Full Text: PDF(206 KB) **IEEE CNF**
Rights and Permissions

Help Contact Us Privacy & :

Indexed by Inspec®

Sign in

Google

Web Images Video News Maps **more »**

"message integrity" "authentication value" "che **Search** Advanced Search
Preferences

Web Results **1** - **3** of about **4** for "**message integrity**" "**authentication value**" "**checking integrity**" **1999**. (0.3

Tip: Try removing quotes from your search to get more results.

Roxen Community: RFC 1477 IDPR as a Proposed Standard ()
IDPR control messages must carry a non-null integrity/**authentication value**. We recommend that control **message integrity**/authentication be based on a digital **...**
community.roxen.com/developers/idocs/rfc/rfc1477.html - 44k - Supplemental Result -
Cached - Similar pages

Integrity check in a communication system - Patent 7009940
1999), 3rd Generation Partnership; Technical Specification Group Services **...** the transmitting party computes a message **authentication value** based on the **...**
www.freepatentsonline.com/7009940.html - 79k - Supplemental Result -
Cached - Similar pages

[PDF] GlobalPlatform Card Specification 2.2.0.7
File Format: PDF/Adobe Acrobat - View as HTML
Recipients of this document are invited to submit, with their comments, notification of any relevant. patent rights or other intellectual property rights of **...**
www.win.tue.nl/pinpasjc/docs/GPCardSpec_v2.2.pdf - Supplemental Result - Similar pages

In order to show you the most relevant results, we have omitted some entries very similar to the 3 already displayed.
If you like, you can repeat the search with the omitted results included.

"message integrity" "authentication v Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google